НАЦІОНАЛЬНИЙ ТЕХНІЧНИЙ УНІВЕРСИТЕТ УКРАЇНИ
«КИЇВСЬКИЙ ПОЛІТЕХНІЧНИЙ ІНСТИТУТ ім. Ігоря
СІКОРСЬКОГО» ФІЗИКО-ТЕХНІЧНИЙ ІНСТИТУТ

Звіт з виконання комп’ютерного практикуму №3

Дослідження криптографічних протоколів систем WebMoney, PayPal

Виконали студенти групи ФІ-32мн
Пелешенко Любов,
Панасюк Єгор,
Маринін Іван Павло
Перевірила: Селюх П.В.

Київ — 2024

Мета роботи: „Дослідження особливостей реалізації криптографічних механізмів платіжних систем”.

Завдання на лабораторну роботу Група 1. Дослідити особливості реалізації криптографічних протоколів, а також особливості роботи з електронними гаманцями систем WebMoney та PayPal. Звіт має містити детальний опис проведеного дослідження особливостей реалізації криптографічних механізмів протоколів систем WebMoney та PayPal. Також звіт має містити загальні теоретичні відомості побудови платіжних систем та їх основні характеристики (специфікація SET), зокрема систем мікроплатежів, таких як Payword та Micromint, та протоколи електронних грошей. Для кожної наведеної системи або протоколу необхідно обґрунтувати його захищеність та вибір криптографічних примітивів.

Загальні теоретичні відомості про платіжні системи

Платіжна система — це сукупність інструментів, процедур, правил і технічної інфраструктури, яка забезпечує перерахування коштів між учасниками (покупцями, продавцями, фінансовими установами тощо). Платіжні системи виконують важливу роль у фінансовій сфері, забезпечуючи швидкі, надійні та ефективні транзакції.

Основні характеристики платіжних систем:

1. **Безпека** — забезпечення конфіденційності, автентифікації, цілісності даних і захисту від шахрайства.
2. **Продуктивність** — здатність обробляти великий обсяг платежів за короткий час.
3. **Надійність** — безперебійна робота системи, резервування даних і доступність.
4. **Масштабованість** — можливість розширення системи при збільшенні кількості учасників чи транзакцій.
5. **Універсальність** — підтримка різних видів платіжних інструментів, валют і платформ.

Специфікація SET (Secure Electronic Transaction)

SET — це протокол безпеки для здійснення електронних платежів у мережі Інтернет. Основною метою SET є забезпечення захисту конфіденційності даних карток і транзакцій.

Основні особливості SET:

1. **Конфіденційність** — використання шифрування для захисту даних.
2. **Автентифікація учасників** — підтвердження особистості продавця та покупця через цифрові сертифікати.
3. **Цілісність даних** — гарантія, що дані не будуть змінені під час передавання.
4. **Незаперечність** — підтвердження факту здійснення транзакції учасниками.

Принцип роботи SET:

- Покупець і продавець отримують сертифікати від довіреного центру сертифікації.
- Транзакція шифрується через алгоритми **RSA** та **DES**.
- Банк, продавець і покупець обмінюються підписаними даними, що забезпечує захищену обробку платежів.

Системи мікроплатежів

Мікроплатежі — це системи для здійснення дрібних фінансових транзакцій (зазвичай менше 1$). Вони ефективні для продажу цифрового контенту, доступу до інформації або невеликих послуг.

1. Payword

Payword є системою мікроплатежів, що ґрунтується на **засвідчених ланцюжках хешів**.

Принцип роботи:

1. **Реєстрація** — користувач реєструється у банку або провайдера мікроплатежів.
2. **Створення ланцюга** — клієнт генерує ланцюжок хешів: $h_n, h_{n-1} = H(h_n), \ldots, h_0$ де H — хеш-функція.
3. **Передплата** — клієнт передає продавцю h_0, який є «коренем» ланцюга, а банк підтверджує його дійсність.
4. **Оплата** — при кожному мікроплатежі клієнт передає наступний елемент ланцюга h_i, а продавець перевіряє його через хешування.
5. **Підсумкова верифікація** — продавець відправляє ланцюжок у банк для зарахування коштів.

Переваги:

- Ефективність та низькі витрати на обчислення.
- Простота для дрібних платежів.

Недоліки:

- Локальність використання ланцюга хешів.
- Обмежена кількість платежів у межах одного ланцюга.

2. Micromint

Micromint — система мікроплатежів, що ґрунтується на використанні **монет** (token), які є хешованими значеннями.

Основні принципи:

1. **Генерація монет** — банк генерує монети шляхом багаторазового застосування хеш-функції.
2. **Верифікація монет** — покупець отримує монети від банку, а продавець перевіряє їх справжність через хешування.
3. **Використання монет** — для кожного платежу покупець передає продавцю набір монет, які не потребують додаткової автентифікації.

Переваги:

- Швидка верифікація монет.
- Можливість попереднього завантаження монет для офлайн-розрахунків.

Недоліки:

- Необхідність захисту від дублювання монет.
- Обмежена кількість монет для транзакцій.

Протоколи електронних грошей

Електронні гроші — це цифровий аналог готівкових коштів, які можна передавати в електронному вигляді без використання банківських рахунків.

Основні протоколи електронних грошей:

1. **Blind Signature (сліпі підписи)**:
    - Засновані на криптографічних підписах, де банк підписує «сліпий» запит користувача.
    - Покупець отримує підписаний токен, що є еквівалентом електронних грошей.
2. **Електронні чекові системи**:
    - Генерація чеків із цифровим підписом клієнта.
    - Банк перевіряє підпис і списує кошти з рахунку клієнта.
3. **Smart Card (розумні картки)**:
    - Картки, що містять чіп для збереження електронних грошей.
    - Транзакції відбуваються безпосередньо між картками.

Система **Payword** має добре продуману архітектуру, яка забезпечує безпеку дрібних фінансових транзакцій, використовуючи ефективні криптографічні примітиви. Нижче наведено обґрунтування її захищеності та вибору криптографічних компонентів.

Основні криптографічні примітиви в Payword:

1. **Криптографічні хеш-функції**:
    - **Призначення**: Хеш-функції використовуються для генерації хеш-ланцюжка $h_n, h_{n-1},..., h_0$, де $h_i = H(h_{i+1})$. Цей механізм є основою системи Payword.
    - **Властивості**:
        - **Однонаправленість (one-way)**: Відзначення елементів ланцюжка можливе лише у напрямку від h_n до h_0, що унеможливлює відновлення попереднього елемента h_{i+1} із h_i .
        - **Стійкість до колізій**: Складність знайти два різних $h_i \neq h_j$, які дають один і той самий хеш $H(h_i) = H(h_j)$, забезпечує надійність перевірки.
2. **Цифрові підписи (Digital Signatures)**:
    - **Призначення**: Використовуються для підпису кореневого значення h_0, яке передається від клієнта до продавця. Банк підтверджує дійсність h_0 через перевірку цифрового підпису клієнта.
    - **Властивості**:
        - **Незаперечність**: Підпис гарантує, що тільки клієнт міг підписати h_0.
        - **Цілісність**: Якщо значення h_0 змінено, підпис стає недійсним.
3. **Симетричне шифрування (опціонально)**:
    - Може використовуватися для захисту конфіденційності обміну даними між клієнтом, продавцем і банком.

Обґрунтування захищеності Payword

1. **Безпека хеш-ланцюжка**:
    - Генерація хеш-ланцюжка ґрунтується на криптографічних хеш-функціях, таких як **SHA-256** або **SHA-3**, які забезпечують стійкість до інверсії та колізій.

- Оскільки хеш-ланцюжок генерується заздалегідь, наступний елемент h_{i+1} не можна відновити з h_i. Це унеможливлює шахрайство з боку продавця, оскільки він не може "створити" додаткові платежі.

2. **Захист від повторного використання платежів**:
   - Кожен елемент хеш-ланцюжка використовується лише один раз, а продавець може перевірити його дійсність через обчислення хеш-функції $h_i = H(h_{i+1})$. Це гарантує, що жоден елемент не може бути використаний повторно.
3. **Довірений банк**:
   - Перед початком транзакцій банк перевіряє дійсність цифрового підпису клієнта та кореневого значення h_0. Продавець може бути впевнений, що h_0 дійсний, оскільки його підтверджено довіреним банком.
4. **Мінімізація ризику компрометації**:
   - Навіть якщо хтось отримує доступ до одного елемента h_i, це не дає змоги визначити попередні елементи ланцюжка (h_{i+1}, h_{i+2}…).
5. **Ефективність і безпека обчислень**:
   - Використання хеш-функцій робить Payword ефективним у порівнянні з методами, які потребують багаторазових операцій шифрування чи підпису.
   - Цифровий підпис потрібен лише для кореневого значення h_0, що мінімізує криптографічні витрати.

Вибір криптографічних примітивів

1. **Хеш-функція (SHA-256/SHA-3)**:
   - Забезпечує високу швидкість обчислень і надійність.
   - Стійка до сучасних атак (навіть квантових, якщо використовується SHA-3).
2. **Цифрові підписи (RSA або ECDSA)**:
   - RSA (2048 біт) або ECDSA (256 біт) забезпечують незаперечність і цілісність даних.
   - Використання ECDSA може бути більш ефективним через меншу довжину ключів і швидші обчислення.
3. **Симетричне шифрування (AES-256)**:
   - Для захисту каналу передачі даних між учасниками може використовуватись AES, що забезпечує високий рівень безпеки та ефективність.

Потенційні вразливості та їх нейтралізація

1. **Можливість підміни кореневого хеша (h_0)**:
    - Нейтралізується за допомогою цифрового підпису клієнта.
2. **Повторне використання платежів**:
    - Хеш-ланцюжок дозволяє використовувати кожен елемент лише один раз, а продавець перевіряє його дійсність перед прийняттям.
3. **Підробка хеш-ланцюжка**:
    - Неможлива через стійкість хеш-функцій до інверсії та колізій.

Обґрунтування захищеності Micromint

1. Генерація монет

У системі Micromint банк генерує монети, використовуючи обчислювально складні криптографічні операції. Кожна монета є результатом хешування, наприклад:

- Монета c_i є валідною, якщо $H(c_i)$ відповідає певному шаблону, наприклад, починається із заданої кількості нулів.

Цей процес гарантує:

- **Одночасне забезпечення унікальності та складності генерування монет**: Банк має обчислювальні ресурси для створення токенів, які відповідають умовам, а зловмисник не може легко підробити монети через високу складність обчислень.

2. Перевірка монет

Продавець або банк перевіряє кожну монету через обчислення хеш-функції. Якщо результат $H(c_i)$ відповідає шаблону, монета визнається дійсною.

- **Швидка верифікація**: Операція перевірки займає значно менше часу, ніж генерація монет.
- **Мінімізація дублювання**: Кожна монета є унікальною завдяки властивостям хеш-функцій.

3. Захист від дублювання монет

Система використовує унікальність хеш-функцій для запобігання повторного використання монет. Кожна монета може бути використана лише один раз, оскільки після її перевірки банк позначає її як використану.

- **Централізована база даних** у банку відстежує вже використані монети, що унеможливлює їх повторну легалізацію.

4. Стійкість до атак:

- **Підробка монет**: Зловмисник не може створити дійсну монету без знання алгоритму генерації та обчислювальної потужності, необхідної для задоволення умов шаблону.
- **Використання чужих монет**: Навіть якщо монета передана іншій особі, банк перевіряє її дійсність та відстежує її статус.

Вибір криптографічних примітивів

1. **Криптографічні хеш-функції (SHA-256/SHA-3)**:
    - **Причини вибору**:
        - Висока швидкість обчислень.
        - Стійкість до сучасних атак на хеш-функції, таких як атаки колізій чи другої передобрази.
        - Надійний рівень безпеки навіть у випадку квантових обчислень (особливо для SHA-3).
2. **Шаблони перевірки монет**:
    - Банк задає шаблон (наприклад, монета має починатися з kkk-кількості нулів), який визначає складність генерування монет.
    - Використання таких умов дозволяє налаштовувати баланс між безпекою та обчислювальними витратами.
3. **Симетричне шифрування (опціонально)**:
    - Для захисту передачі монет між клієнтом, продавцем і банком може використовуватися AES-256. Це гарантує конфіденційність переданих токенів.

Порівняння з іншими системами

1. **Ефективність**:
    - На відміну від Payword, де кожна транзакція вимагає перевірки частини хеш-ланцюжка, в Micromint перевірка здійснюється миттєво через обчислення одного хеша.
2. **Обчислювальні витрати**:
    - Генерація монет у Micromint може бути ресурсоємною, але перевірка монет надзвичайно швидка. Це робить систему ефективною для мікроплатежів з великою кількістю транзакцій.
3. **Простота**:
    - Система Micromint простіша в реалізації порівняно з SET або іншими протоколами, оскільки не вимагає використання цифрових підписів для кожної транзакції.

Потенційні вразливості та їх вирішення

1. **Колізії хеш-функцій**:
    - Використання сучасних хеш-функцій (SHA-3) значно зменшує ймовірність колізій.
2. **Використання дублікованих монет**:

    - Усі монети реєструються банком, а їх повторне використання унеможливлюється шляхом перевірки унікальності.
3. **Можливість компрометації бази даних банку**:
    - Резервування та шифрування бази даних забезпечують стійкість до атак на сервер.

Основні криптографічні механізми WebMoney

1. **Цифрові підписи (Digital Signatures)**:
    - Використовуються для підтвердження автентичності повідомлень і забезпечення незаперечності транзакцій.
    - У WebMoney застосовується асиметрична криптографія:
        - Кожен користувач має пару ключів: **приватний** (для підпису транзакцій) та **публічний** (для перевірки підпису).
    - Алгоритми: традиційно використовуються RSA або ECDSA (залежно від версії та рівня облікового запису).
2. **Шифрування даних**:
    - Для захисту даних, що передаються між клієнтом і сервером, використовується симетричне шифрування.
    - Протокол TLS (Transport Layer Security) забезпечує шифрування всіх даних під час сеансу зв’язку.
    - Симетричний алгоритм: **AES (Advanced Encryption Standard)**, зазвичай із довжиною ключа 256 біт.
3. **Хешування**:
    - Хеш-функції використовуються для перевірки цілісності даних і створення підписів.
    - Основний алгоритм хешування: **SHA-256** (або його варіанти залежно від реалізації).
    - Використовується для забезпечення:
        - Непідробності підписів.
        - Контролю автентичності та цілісності переданих даних.
4. **Одноразові паролі (OTP)**:
    - Для додаткової автентифікації користувачів можуть застосовуватися одноразові паролі (наприклад, для входу в систему або підтвердження операцій).
    - Механізм базується на алгоритмах, таких як **TOTP (Time-based One-Time Password)**, що забезпечує короткострокову дійсність пароля.
5. **Ключові файли (Key Files)**:
    - WebMoney використовує унікальний файл ключів, створений під час реєстрації користувача.
    - Файл зберігає приватний ключ для підпису транзакцій.
    - Цей файл додатково захищений паролем користувача, що ускладнює доступ до нього у разі компрометації.
6. **Електронні сертифікати**:
    - Кожен обліковий запис має унікальний сертифікат, який пов’язує його з відповідним ключем.
    - Цей сертифікат використовується для верифікації особистості учасника транзакції.

7. **Додаткові механізми безпеки**:
    - **2FA (двохфакторна автентифікація)**: для входу та підтвердження операцій можна використовувати SMS-коди, мобільні додатки чи апаратні токени.
    - **Ліміти транзакцій**: встановлюються для кожного облікового запису як додатковий захист від шахрайства.

Особливості реалізації криптографічних механізмів WebMoney

1. **Автентифікація користувачів**:
    - Автентифікація проводиться за допомогою:
        - Приватного ключа користувача (зберігається у файлі ключів або на апаратному носії).
        - Додаткових методів, таких як паролі або OTP.
    - Якщо файл ключів втрачається, користувач має пройти процедуру відновлення доступу через службу підтримки.
2. **Підпис транзакцій**:
    - Кожна транзакція підписується приватним ключем користувача. Підпис додається до повідомлення і передається серверу WebMoney.
    - Сервер перевіряє підпис за допомогою публічного ключа, збереженого в сертифікаті користувача.
3. **Конфіденційність даних**:
    - Усі дані, що передаються через мережу, шифруються за допомогою TLS.
    - Це захищає транзакції від перехоплення та несанкціонованого доступу до фінансових даних.
4. **Захист від повторного використання повідомлень**:
    - Використовується унікальний ідентифікатор для кожного повідомлення (nonce).
    - Сервер відхиляє дублікати повідомлень, що запобігає атакам повторного використання (replay attacks).
5. **Контроль цілісності даних**:
    - Передача даних між клієнтом і сервером супроводжується обчисленням хешу.
    - Сервер перевіряє хеш отриманих даних, щоб переконатися в їхній цілісності.
6. **Мультиплатформеність**:
    - WebMoney підтримує різні платформи (десктопні програми, веб-інтерфейси, мобільні додатки).

- На мобільних пристроях реалізується захист за допомогою біометричної автентифікації (відбитки пальців або розпізнавання обличчя).

Потенційні вразливості та їх нейтралізація

1. **Компрометація приватного ключа**:
   - Захист забезпечується паролем до файлу ключів або зберіганням ключів на апаратному токені.
   - Додатково використовується двофакторна автентифікація.
2. **Фішингові атаки**:
   - WebMoney використовує сертифікати SSL для автентифікації серверів.
   - Користувачам рекомендується перевіряти URL-адресу та сертифікати під час входу.
3. **Вразливості в передачі даних**:
   - Шифрування TLS захищає від атак типу «людина посередині» (MITM).
4. **Атаки на верифікацію транзакцій**:
   - Використання унікальних ідентифікаторів транзакцій (nonce) і хешування запобігає повторним атакам.

Основні криптографічні механізми PayPal

1. **Шифрування TLS (Transport Layer Security)**:
    - Забезпечує конфіденційність і захист даних під час їхньої передачі між клієнтом і сервером.
    - Використовується найсучасніша версія TLS (зазвичай TLS 1.3), яка включає такі елементи:
        - Алгоритми шифрування: **AES (Advanced Encryption Standard)** з довжиною ключа 256 біт.
        - Криптографічні протоколи обміну ключами: **ECDHE (Elliptic Curve Diffie-Hellman Ephemeral)**.
        - Алгоритми хешування: **SHA-256** або **SHA-3** для забезпечення цілісності даних.
2. **Цифрові підписи (Digital Signatures)**:
    - Використовуються для забезпечення автентичності даних і незаперечності транзакцій.
    - Алгоритми: **RSA** (2048/3072/4096 біт) або **ECDSA (Elliptic Curve Digital Signature Algorithm)**.
    - Підписування даних відбувається на сервері PayPal, а клієнти перевіряють підписи для підтвердження справжності інформації.
3. **Автентифікація користувачів**:
    - Використовуються декілька рівнів автентифікації:
        - **Парольний захист**: користувачі вводять логін і пароль для входу.
        - **Двофакторна автентифікація (2FA)**: включає OTP (одноразові паролі) через SMS, електронну пошту або мобільний додаток (наприклад, Google Authenticator).
        - **Біометрична автентифікація**: у мобільних додатках доступна автентифікація за допомогою відбитків пальців або розпізнавання обличчя.
4. **Шифрування даних у сховищі**:
    - Конфіденційна інформація (наприклад, номери кредитних карток) зберігається в зашифрованому вигляді.
    - Використовується **AES-256** для шифрування даних у сховищах.
5. **Одноразові токени (OAuth 2.0)**:
    - Використовуються для автентифікації під час інтеграції PayPal з іншими системами (API).
    - Токени є тимчасовими, що зменшує ризик компрометації.
    - Шифрування токенів гарантує їхню конфіденційність і неможливість підробки.
6. **Хешування даних**:
    - Для перевірки цілісності повідомлень використовується хешування з алгоритмами **SHA-256** або **SHA-3**.

    - Хешування паролів клієнтів у базах даних: паролі хешуються з використанням сучасних функцій, таких як **bcrypt**, з додаванням солі (salt).
7. **Протоколи боротьби з шахрайством**:
    - Використовуються криптографічні механізми для аналізу транзакцій у реальному часі:
        - Генерація унікальних ідентифікаторів транзакцій (nonce).
        - Криптографічний захист повідомлень для запобігання атакам повторного використання (replay attacks).
8. **Захист API**:
    - Для інтеграцій через PayPal API реалізовані такі механізми:
        - **Електронні сертифікати SSL**: забезпечують автентичність запитів до API.
        - **OAuth 2.0**: дозволяє обмежити доступ до ресурсів на основі токенів доступу.

Особливості реалізації криптографічних механізмів

1. **Безпечна передача даних**:
    - Вся інформація передається через HTTPS з використанням TLS.
    - TLS забезпечує захист від атак типу «людина посередині» (MITM) і перехоплення даних.
2. **Маскування платіжних даних**:
    - Платіжна інформація клієнтів (номери карток, банківські реквізити) не передається продавцю. Замість цього використовується унікальний токен або ідентифікатор транзакції.
3. **Автоматична перевірка транзакцій**:
    - Використання криптографічних механізмів для автоматичної перевірки справжності транзакцій на стороні продавців через IPN (Instant Payment Notification) або Webhooks.
4. **Стійкість до атак повторного використання (Replay Attacks)**:
    - Для кожної транзакції генерується унікальний ідентифікатор (nonce), який робить повторну передачу того ж повідомлення недійсною.
5. **Захист API-ключів**:
    - API-ключі шифруються і зберігаються у спеціалізованих апаратних модулях безпеки (HSM).

Потенційні вразливості та їх нейтралізація

1. **Фішингові атаки**:
    - PayPal використовує сертифікати SSL для автентифікації серверів.
    - Користувачів інформують про необхідність перевірки домену перед введенням даних.
2. **Компрометація облікових записів**:
    - Використання 2FA значно зменшує ризик отримання доступу до облікового запису при компрометації пароля.
3. **Атаки на сервери**:
    - Усі конфіденційні дані зберігаються в зашифрованому вигляді.
    - Реалізовані багаторівневі системи моніторингу доступу до серверів.
4. **Атаки на токени доступу**:
    - Використання OAuth 2.0 з короткоживучими токенами та їх шифрування зменшує ризик компрометації.

Переваги криптографічних механізмів PayPal

1. **Високий рівень безпеки**:
    - Шифрування TLS і сучасні алгоритми забезпечують захист даних навіть у разі перехоплення.
2. **Гнучкість інтеграції**:
    - Протоколи OAuth 2.0 та API дозволяють легко інтегрувати PayPal з іншими сервісами, не знижуючи рівень безпеки.
3. **Маскування платіжних даних**:
    - Використання токенів гарантує, що платіжні дані клієнтів залишаються конфіденційними.
4. **Прозорість і легкість використання**:
    - Незважаючи на складну криптографічну інфраструктуру, PayPal пропонує зручний інтерфейс для користувачів і розробників.

Висновки:

Порівняння PayPal і WebMoney з точки зору криптографічних механізмів.

Аспект	PayPal	WebMoney
Шифрування передачі даних	Використання TLS 1.3 із алгоритмами AES-256 і ECDHE.	TLS із AES-256 для захисту зв’язку між клієнтом і сервером.
Цифрові підписи	Використання RSA/ECDSA для забезпечення автентичності даних і транзакцій.	Приватний ключ користувача зберігається у файлі ключів або на апаратному токені.
Хешування	SHA-256/SHA-3 для цілісності повідомлень.	SHA-256 для хешування паролів і перевірки транзакцій.
Двофакторна автентифікація	2FA (OTP через SMS, мобільні додатки, біометрія).	2FA із використанням кодів, отриманих через SMS або мобільний додаток.
Одноразові токени	OAuth 2.0 для інтеграції API, короткоживучі токени.	Генерація унікальних ідентифікаторів транзакцій для запобігання повторним атакам.